

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X  
PURE POWER BOOT CAMP, INC., et. al., :  
 :  
 Plaintiffs, :  
 :  
 -against- : 08 Civ. 4810  
 : (JGK) (THK)  
 :  
 WARRIOR FITNESS BOOT CAMP, LLC, et. al, : **Report and**  
 : **Recommendation**  
 :  
 Defendants. :  
-----X  
**FROM: THEODORE H. KATZ, United States Magistrate Judge.**  
**TO: HON. JOHN G. KOELTL, United States District Judge.**

Plaintiffs bring this action seeking an injunction and damages, accusing Defendants of (1) stealing Plaintiffs' business model, customers, and internal documents, (2) breaching employee fiduciary duties, and (3) infringing Plaintiffs' trademarks, trade-dress, and copyrights. This case was referred to this Court for general pretrial management.

Currently before the Court is Defendants' motion to preclude the use or disclosure of thirty-four of Defendant Alexander Fell's ("Fell") e-mails, obtained by Lauren Brenner ("Brenner"), the principal and owner of the Plaintiff corporations ("Plaintiffs"), and Fell's former employer. Defendants also seek an order requiring the e-mails' immediate return and attorneys' fees and costs.

The parties have fully briefed the issues, and, on July 18, 2008, the Court heard oral argument on the motion. Although the

preclusion of evidence as a discovery sanction might normally be a non-dispositive matter for the Court to decide as part of its general pretrial supervision of a case, in this case, because of the potentially dispositive nature of the instant motion and its evidentiary implications for matters before the District Court, the District Court has requested that this Court provide a Report and Recommendation containing findings of fact, an analysis of the legal issues, and a discussion of the range of possible remedies available to the Court.

As explained in greater detail below, the Court concludes that Brenner accessed Fell's e-mails without authorization, in what would be a violation of the Stored Communications Act, 18 U.S.C. § 2707, had a cause of action been brought pursuant to that statute. The Court also concludes that, pursuant to its inherent equitable authority over the litigation process, the e-mails should be precluded, in part or in whole. Finally, the Court concludes that one e-mail is protected by the attorney-client privilege and should be returned to Defendants.

#### **BACKGROUND**

Fell was hired by Brenner in August of 2005, and worked at Pure Power Boot Camp ("PPBC"), a physical fitness center, until March 16, 2008, when Brenner fired him. On April 1, 2008, Defendant Ruben Belliard ("Belliard"), who is now Fell's business partner, and was also employed at PPBC, entered Brenner's office

when she was not there, stayed there for half an hour, called Brenner on her office telephone, and quit.<sup>1</sup> A few months before he left his employ at PPBC, Belliard entered Brenner's office, again when she was not present, removed a copy of a restrictive covenant he had signed, and shredded it. (See Belliard Aff. ¶ 31.) Soon after Fell and Belliard left PPBC, they opened a competing fitness center, Warrior Fitness Boot Camp ("WFBC"), together with their girlfriends - Defendants Jennifer Lee ("Lee") and Nancy Baynard ("Baynard").

After Fell and Belliard were no longer working at PPBC, Brenner, on April 28, 2008, and for a week thereafter, accessed and printed e-mails from three of Fell's personal accounts: "kappamarine@hotmail.com" ("Hotmail account"), "kappamarine@gmail.com" ("Gmail account"), and "alex@warriorfitnessbootcamp.com" ("WFBC account"). (See Brenner July 10 Aff. ¶ 22; see also Exhibit ("Ex.") A, annexed to Declaration of Daniel Schnapp, Esq. ("Schnapp Decl."), dated July 1, 2008, E-mails 1-34; Transcript of Oral Argument, dated July 18, 2008 ("Tr."), at 14-15.)<sup>2</sup>

---

<sup>1</sup> Brenner alleges that Belliard stole PPBC's client list and other items while he was in her office. (See Affidavit of Lauren Brenner, dated July 10, 2008 ("Brenner July 10 Aff."), ¶ 16.) Belliard denies he stole anything. (See Affidavit of Rubin Belliard, dated July 29, 2008 ("Belliard Aff."), ¶ 33.)

<sup>2</sup> All references to e-mails are to the e-mails annexed to Schnapp's Declaration.

Brenner states that she was able to access Fell's Hotmail account because he left his username and password information stored on PPBC's computers, such that, when the Hotmail website was accessed, the username and password fields were automatically populated. (See Brenner July 10 Aff. ¶ 13.) She also alleges that Fell gave his username and password to another PPBC employee, Elizabeth Lorenzi, so that she could check on an Ebay sale he was conducting. (See Affidavit of Elizabeth Lorenzi, dated July 10, 2008 ("Lorenzi Aff."), ¶¶ 3, 6.) Plaintiffs allege, and Fell does not deny, that Fell accessed his Hotmail account while at work at PPBC, which is how his username and password came to be stored on the company's computers. At oral argument, Plaintiffs admitted that Brenner was able to access Fell's Gmail account because the username and password for the Gmail account were sent to Fell's Hotmail account, which Brenner accessed. (See Tr. at 17.) Brenner also explained that she was able to access Fell's WFBC account by making a "lucky guess" at his password, which turned out to be the same password he used for his other accounts. (See id. at 15-16.)

Plaintiffs have an Employee Handbook which explicitly addresses e-mail access on company computers. It states:

"e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system. This includes the use of personal e-mail accounts on Company equipment. The Company, in its discretion as owner of the E-Mail system, reserves the right to review, monitor, access, retrieve, and delete any

matter stored in, created on, received from, or sent through the system, for any reason, without the permission of any system user, and without notice."

(Ex. A, annexed to Supplemental Affidavit of Lauren Brenner, dated June 6, 2008 ("Brenner June 6 Aff.") (emphasis added).) An additional part of the policy states: "Internet access shall not be utilized for shopping or for conducting other transactions or personal business matters." (Id.) Plaintiffs have not conducted a forensic evaluation of the company computers to determine what e-mails Fell actually received, sent through, read, or accessed from the company's computers. (See Tr. at 22.)

E-mails 1-26 and 28, were obtained from Fell's Hotmail account; of those, E-mails 1-13 and 16 are dated prior to March 16, 2008, the date Fell stopped working at PPBC. E-mails 27, 29-31, 33, and 34 were obtained from Fell's Gmail account. E-mail 32 was obtained from Fell's e-mail account at WFBC.

Fell states in his affidavit that all of the e-mails were drafted or received on his own home computer. (See Affidavit of Alex Fell, dated July 1, 2008 ("Fell Aff."), ¶ 5.) Fell denies that he ever gave his Hotmail information to anyone at PPBC. (See id. ¶ 4.) Fell does not deny, however, that he may have viewed some of his e-mails on PPBC's computers while he was working there.

While it is not possible to determine from the submissions when the e-mails were read, they do indicate the date and time they were sent. E-mails sent by Fell indicate that they were sent at

all times during the day, on various days of the week. For example, E-mail 4 shows that Fell sent a message on Monday, February 11, 2008 at 3:09 p.m. in the afternoon. E-mail 6 was sent on Wednesday, February 20, 2008 at 2:37 p.m. On Thursday, February 28, 2008, Fell sent E-mail 9 at 3:35 in the morning. E-mail 16 was sent the day before Fell was fired, Saturday, March 15, 2008 at 5:06 p.m. Each of these e-mails relates to, or discusses his efforts to set up his competing business - WFBC.<sup>3</sup>

Plaintiffs have relied heavily upon the e-mails and have considered them critical to their case. The e-mails provide a detailed picture of Fell's and Belliard's efforts to set up WFBC before they left PPBC, the work that Lee and Baynard did to support those efforts - including recruiting PPBC clients for WFBC while they themselves were still clients of PPBC, and the fallout after Fell and Belliard left PPBC. For example, E-mail 29 is a candid admission that Belliard shredded his non-compete contract with PPBC, a fact Defendants attempted to avoid revealing during prior state court proceedings. (See Ex. B annexed to Declaration of Daniel Schnapp, dated July 3, 2008, transcript of proceedings before Hon. Helen Freedman, New York Supreme Court, dated May 8, 2008 ("NY Tr."), at 28.) E-mail 21 shows a dramatic expansion of

---

<sup>3</sup> Fell makes a general claim that he never did any work related to WFBC while he was at PPBC or on PPBC computers. (See Fell Aff. ¶ 6.) However, he has not provided his PPBC work schedule, so there is no way to confirm whether or not he was at PPBC when he sent any of these e-mails.

WFBC's customer list, and includes a large number of former PPBC clients and their e-mail addresses, which Plaintiffs rely upon to show that Belliard stole PPBC's client list. (See Declaration of Richard Herzfeld, Esq., dated July 11, 2008, ¶ 25.)

Some of the e-mails were sent to, or received from, Defendants' attorneys. (See E-mails 12, 13, 14, 28.)<sup>4</sup> E-mail 13 was sent from a legal assistant at Fox Rothschild, Defendants' counsel, attaching an IRS document containing WFBC's employer ID number. E-mail 14, from the same paralegal, attached WFBC's Articles of Organization, and informed Fell that they were filed with the State of New York. E-mail 28 is from an attorney at Fox Rothschild, and appears to have been printed from Fell's "sent" file; it is part of an e-mail chain consisting of back-and-forth e-mails from the same Fox Rothschild attorney, and contains advice about how to handle telephone calls from Brenner.

When Plaintiffs first filed suit seeking a temporary restraining order and preliminary injunction in state court, they used the challenged e-mails as exhibits. However, at the time the e-mails were provided to Defendants, the bottom part of the page, which shows when an e-mail was printed, was obscured or removed.

---

<sup>4</sup> Defendants did not include "E-mail 12" in their submissions, although it is described and referred to in the pleadings. (See Defendants' Memorandum of Law in Support of Their Motion for an Order Precluding the Use or Disclosure of Specific Emails ("Defs.' Mem."), at 7.) According to Defendants, E-mail 12 is a privileged e-mail from Defendants' attorneys. (See id.)

(See all e-mails in Ex. A.) Defendants allege that this amounts to spoliation of evidence. In response, during oral argument, Plaintiffs stated that they had the original copies of the e-mails, showing when they were printed, and agreed to provide unredacted copies to Defendants. (See Tr. at 33-34.)

#### **DISCUSSION**

Defendants seek the preclusion and return of Fell's e-mails, claiming that Brenner violated the Electronic Communications Privacy Act, 18 U.S.C. § 2510 ("ECPA"), the Stored Communications Act, 18 U.S.C. § 2707 ("SCA"), and New York Penal Law § 250.05, when she accessed Fell's e-mail accounts. Defendants also argue that some e-mails are protected by attorney-client privilege. Finally, Defendants argue that Plaintiffs' production of the e-mails with the dates on which they were printed obscured, amounts to spoliation of evidence, further justifying preclusion.

Plaintiffs argue that the ECPA and New York Penal Law do not apply, and that, in any event, Fell gave implied consent which authorized Brenner's access. Plaintiffs also argue that the crime-fraud exception to confidentiality should apply not only to any e-mails covered by the attorney-client privilege, but to all the e-mails accessed by Brenner. Finally, Plaintiffs argue that the redaction of the printing dates does not constitute sanctionable spoliation.

It is important to note from the outset, that this is not a



situation in which an employer is attempting to use e-mails obtained from the employer's own computers or systems. Rather, the e-mails at issue here were stored and accessed directly from accounts maintained by outside electronic communication service providers. Furthermore, Defendants have not directly asserted any claims under the statutes they allege Brenner violated, and instead, appeal only to the Court's inherent equitable authority to preclude evidence wrongfully obtained, outside of the litigation process, from being used in the litigation. Thus, while Defendants invoke federal and state law, those laws are invoked solely for the Court to consider as part of the process of weighing the competing equitable considerations raised by the conduct of both sides to this dispute.

#### I. The Statutes

All three of the statutes Defendants rely upon are criminal statutes that also provide relief to aggrieved parties in civil causes of action. Of the three statutes, however, only the Stored Communications Act is applicable.

##### A. The Stored Communications Act

The Stored Communications Act, 18 U.S.C. § 2701, et. seq. ("SCA"), part of the Wiretap Act, provides in part:

- (a) Offense.--Except as provided in subsection
- (c) of this section whoever--
- (1) intentionally accesses without authorization a facility through which an electronic communication service is provided;
- or

(2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

18 U.S.C.A. § 2701 (emphasis added). The Act "aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications." In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 507 (S.D.N.Y. 2001) (citing Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000)). Thus, a person violates the SCA if she accesses an electronic communication service, or obtains an electronic communication while it is still in electronic storage, without authorization.

"Electronic storage," defined in an earlier part of the Wiretap Act is: "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication . . . ." 18 U.S.C. §§ 2510(17), 2711(1) (definitions of Wiretap Act applicable to Stored Communications Act).

The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider's systems after it has been delivered, as opposed

to e-mail stored on a personal computer, is a stored communication subject to the SCA. See United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) (describing in detail the nature of e-mail, and concluding that "the term 'electronic communication' includes transient electronic storage that is intrinsic to the communication process for such communications."); see also Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3rd Cir. 2003) (holding that e-mail stored on the defendant's system was subject to the SCA); cf. Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 n.1 (2d Cir. 2005) (finding unpersuasive the argument that an e-mail in storage is not an "electronic communication").

In a case analogous to this one, Baily v. Bailey, No. 07 Civ. 11672, 2008 WL 324156 (E.D. Mich. Feb. 6, 2008), the ex-husband defendant installed a keystroke logger on a computer shared by him and his then-wife, which allowed him to learn her password to her Yahoo account (among others), and which he used to access her e-mail directly from her Yahoo account. See id. at \*3. The wife filed suit pursuant to the SCA, as well as under 18 U.S.C. § 2511, the ECPA. See id. The court denied a motion for summary judgment brought by the defendant, who claimed that neither statute applied, and determined that e-mails, "received by the intended recipient where they remain stored by an electronic communication service," are covered by the SCA. Id. at \*6 (citing Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2003)).

In this case, Brenner obtained Fell's username and password to his Hotmail account because he left that information stored on Plaintiffs' computers. She then used that information to go into his Hotmail account, and read and printed his e-mails. Some of those e-mails may have been read by Fell while he was at work, but there is no evidence indicating which e-mails he may have viewed on Plaintiffs' computers, and there is no evidence that the e-mails were downloaded onto PPBC's computers. At most, only e-mails dated prior to his last day of work could have been viewed by him and thus potentially stored on the company's systems.

In any event, Brenner did not use an examination of PPBC's computer's memory to determine what Fell accessed at work. Instead, she logged directly onto Microsoft's Hotmail system where the e-mails were stored, and viewed and printed them directly off of Hotmail's system. She accessed Fell's other accounts in the same manner, and there is no evidence indicating that Fell accessed his Gmail or WFBC accounts at any time while he worked at PPBC. By Plaintiffs' own admission, Brenner obtained the username and password for the Gmail account from Fell's Hotmail account, and made a "lucky guess" that Fell would use the same password for all three accounts, including his WFBC account.

Thus, Brenner accessed three separate electronic communication services, and she obtained Fell's e-mails while they were in storage on those service providers' systems. Either of those

actions, if done without authorization, would be a violation of the SCA. See Wyatt Technology Corp. v. Smithson, No. CV 05-1309 (DT), 2006 WL 5668246, \*9 (C.D. Cal. Aug. 14, 2006) (granting summary judgment in favor of counter-claimant alleging that the plaintiff violated the SCA by accessing the defendant's personal e-mail on a private foreign server, and monitoring the personal e-mail account, without authorization).

B. The Electronic Communications Privacy Act

The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2511 ("ECPA"), creates criminal sanctions and a civil cause of action against persons who "intercept" electronic communications.<sup>5</sup> In the context of unauthorized access to e-mail, the question that courts have struggled with is determining whether one can "intercept" an e-mail that has already been delivered. The Second Circuit has not directly addressed this question, but has discussed the issue in at least one case. See Hall, 396 F.3d at 503 n.1.

---

<sup>5</sup> 18 U.S.C.A. § 2515 reads:

Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

In Hall, the Second Circuit held that the ECPA was applicable to the e-mails at issue because "the case involve[d] the continued receipt of e-mail messages rather than the acquisition of previously stored electronic communication." 396 F.3d at 503 n.1 (emphasis in original). The Circuit was unpersuaded by the defendant's argument that "an 'interception' [as required by the ECPA,] can only occur when messages are in transit," but did not elaborate further. Id. Rather, it factually distinguished the cases cited by the defendant - which held that e-mails no longer in transit cannot be "intercepted." See id. (distinguishing: Fraser, 352 F.3d at 110; United States v. Steiger, 318 F.3d 1039, 1048-49 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 873, 876-79 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 460-64 (5th Cir. 1994)).

Hall is itself factually distinguishable from this case. Hall involved the continued and contemporaneous acquisition of e-mails as part of the ordinary course of the defendant's business - which was the internet communication service provider for the e-mails in question. See id. Here, PPBC is not an internet communications provider, and Brenner did not access the e-mails on a continuous basis, contemporaneous with their transmission. Rather, by the time Brenner viewed the e-mails, they had been delivered to Fell's accounts, and may have already been viewed by him; thus, they were "previously stored electronic communications" - precisely the

situation which Hall relied upon to distinguish the decisions the defendants relied upon in that case. See id.

Other courts which have considered the question of whether accessing an electronic communication that has already been delivered is "intercepted," have found that the ECPA does not apply. See Fraser, 352 F.3d at 113-14 (holding that the defendant did not "intercept" the plaintiff's e-mail by accessing e-mail stored on its central file server, because "an 'intercept' under the ECPA must occur contemporaneously with transmission"); Steiger, 318 F.3d at 1048-49 (declining to suppress evidence obtained by a hacker from defendant's computer, pursuant to the ECPA, because "a contemporaneous interception - i.e., an acquisition during "flight" - is required to implicate the [ECPA] with respect to electronic communications"); Konop, 302 F.3d at 873, 878-80 (noting subsequent changes in the Wiretap Act support the conclusion that accessing a secure website did not constitute an "interception" of an electronic communication under the ECPA, and narrowly defined interception as "contemporaneous interception").

As the court in Bailey explained: "The general reasoning behind these decisions is that based on the statutory definition and distinction between 'wire communication' and 'electronic communication,' the latter of which conspicuously does not include electronic storage, Congress intended for electronic communications in storage to be handled solely by the Stored Communications Act."

Bailey, 2008 WL 324156, at \*4; see also Fraser, 352 F.3d at 113-14 (explaining the statutory interpretation issues). Thus, in those cases which have examined whether the ECPA or the SCA should apply to delivered e-mails, courts have concluded that the SCA, not the ECPA, is the proper statute to apply in situations similar to this case. See Steiger, 318 F.3d at 1049 (noting that "the SCA may apply [in this case] to the extent the source accessed and retrieved any information stored with Steiger's Internet service provider").

Defendants concede that the ECPA has a requirement of contemporaneous interception. (See Tr. at 12.) Nonetheless, Defendants suggest that Brenner's access to Fell's e-mail was "contemporaneous" if it occurred during some undefined, short period of time after the e-mail had been delivered. (See Tr. at 12-13.) However, they have not provided any authority for that proposition, nor have they suggested how long a "contemporaneous time frame" would be. (Id.) In any event, there is no evidence of when Brenner accessed Fell's e-mails, but its clear that the majority of the e-mails were sent or received prior to April 28, 2008, the earliest date that Brenner admits that she accessed and printed them. Additionally, there is no evidence that the later e-mails were intercepted at the same time that they were delivered. Rather, the evidence indicates that Brenner periodically accessed



Fell's e-mail accounts and printed e-mails after they had been delivered.

Applying the definition of "intercept" accepted by the majority of courts to have examined the issue, the Court concludes that Brenner did not access and print Fell's e-mails contemporaneous with their transmission. See Fraser, 352 F.3d at 113-14. Therefore, the Court concludes that Brenner did not violate the ECPA.

C. New York Eavesdropping and Civil Procedure Laws

Defendants argue that Brenner also violated New York's eavesdropping law, and, pursuant to a New York procedural rule, Fell's e-mails should be precluded. New York Penal Law § 250.05 makes it a crime for a person to "unlawfully engage in wiretapping, . . . or intercepting or accessing [an] electronic communication." N.Y. Penal Law § 250.05 (McKinney 2008). New York Civil Practice Law and Rule § 4506 ("CPLR § 4506") states:

"The contents of any overheard or recorded communication, conversation or discussion, or evidence derived therefrom, which has been obtained by conduct constituting the crime of eavesdropping, as defined by section 250.05 of the penal law, may not be received in evidence in any trial, hearing or proceeding before any court . . . ."

N.Y. C.P.L.R. § 4506 (Consol. 2008).

If a party to a civil action seeks preclusion pursuant to § 4506, it must bring a motion "before a justice of the supreme court . . . ." Id. at § 4506(4). In contrast to the federal laws, New

York's rule does not provide a separate civil cause of action, but, rather, is only a vehicle through which evidence may be excluded in an underlying case. See id. It also does not provide for damages, attorneys' fees, costs, or any remedy other than exclusion of the evidence. See id.

There is a notable dearth of state law construing CPLR § 4506. Defendants have not cited, and the Court has not found, any published cases applying CPLR § 4506 to unauthorized access to e-mail. On its face, however, the statute does not appear to apply in this situation. The plain language of the statute seems to limit its application to the contents of an "overheard or recorded communication." CPLR § 4506. Furthermore an aggrieved person is defined as one whose "communication, conversation or discussion was unlawfully overheard or recorded." Id. at § 4506(3)(a). In addition, the statute only makes reference to "telephonic or telegraphic communication[s]," not electronic communications. Id. at § 4506(2)(a). This language seems to limit the application of the statute to communications obtained aurally, rather than to electronic communications such as e-mail.<sup>6</sup>

Furthermore, neither party has briefed the fundamental and more complex issue of whether CPLR § 4506, a rule governing the

---

<sup>6</sup> The Court also notes that Penal Law § 250.05 explicitly includes "electronic communications" while CPLR § 4506 does not, suggesting that e-mails obtained in violation of Penal Law § 250.05 are not subject to exclusion under CPLR § 4506.

exclusion of evidence in New York state courts, ought to be applied by this Court pursuant to Erie R. Co. v. Tompkins, 304 U.S. 64, 58 S. Ct. 817 (1938).<sup>7</sup> Cf. United States v. Canniff, 521 F.2d 565, 568 (2d Cir. 1975) ("Under New York law (which, however, is not controlling in this federal proceeding), [evidence] of a youthful offender adjudication for the purpose of impeachment is prohibited . . . ." (internal citation omitted)).

Ultimately, a determination of the meaning of CPLR § 4506 is unnecessary, and better left to the New York state courts. The Court could preclude use of the e-mails pursuant to the SCA or its inherent authority, without applying CPLR § 4506. Thus, there is no need to resolve the issues of whether CPLR § 4506 is applicable to this action and, if so, whether it mandates the preclusion of the e-mails.

#### D. Authorization

Accessing and obtaining e-mails directly from an electronic communication service provider is a violation of the SCA if done without authorization. Having determined that the SCA is applicable to Brenner's conduct, she therefore may not have violated the SCA if she was authorized to access Fell's e-mail accounts.

Plaintiffs argue that Brenner was authorized to view and print Fell's e-mails, and assert two theories in support of this

---

<sup>7</sup> There are both federal and state law substantive claims in this action.

position. First, Plaintiffs claim that PPBC's e-mail policy put Fell on notice that his e-mails could be viewed by Brenner, and thus he had no expectation of privacy in his Hotmail account. Second, Plaintiffs argue that even if he had an expectation of privacy, Fell, by leaving his username and password on PPBC's computers, gave Brenner implied consent to access his accounts.

Defendants respond by denying that Fell gave PPBC, or any of its agents or employees, authorization to access his accounts, and specifically deny that Fell gave his username and password to Brenner's assistant. Defendants also deny that PPBC had its e-mail policy in place during Fell's employment, and suggest that it is a recent creation by Brenner. (See Tr. at 4-5.) In any event, they argue that it does not cover e-mails sent after Fell left PPBC's employ.

Brenner claims Fell had no expectation of privacy in his e-mails and that Fell gave implied consent to unlimited access to all of Fell's personal e-mail accounts, with no time constraints (not even for the period after Fell's employment at PPBC ended), based on her assertion that Fell accessed his personal Hotmail account, at least once, on Plaintiffs' computer. These arguments have no sound basis in fact, law, or logic.

As an initial matter, Plaintiffs' position is not supported by PPBC's policy. PPBC's e-mail policy - the basis of Plaintiffs' consent defense - is, by its own terms, limited to "Company

equipment." The reservation of rights is explicitly limited to "any matter stored in, created on, received from, or sent through [PPBC's] system."<sup>8</sup> Therefore, it could not apply to e-mails on systems maintained by outside entities such as Microsoft or Google. In addition, there is no evidence that the e-mails in issue were created on, sent through, or received from PPBC's computers. Moreover, Plaintiffs' position makes no distinction between the Hotmail account Fell accessed while at work, and the other accounts, which by all appearances were never accessed by Fell at work, and may not even have existed until after he left PPBC's employ.

Plaintiffs' position - that Brenner was authorized to access Fell's e-mails on his personal e-mail service providers' systems through his implied consent - also has no support in the law. To understand the basis of Plaintiffs' argument, and why it has no legal support, it is important to first understand the framework within which the typical employee e-mail case usually arises. Courts have routinely found that employees have no reasonable expectation of privacy in their workplace computers, where the

---

<sup>8</sup> Even the case Plaintiffs rely upon, in support of the argument that Fell waived his right to privacy in his Hotmail account, acknowledges that an employer's e-mail policy is limited only to e-mails viewed by employees while at work. See Scott v. Beth Israel Med. Ctr. Inc., 17 Misc.3d 934, 938, 847 N.Y.S.2d 436, 440 (N.Y. Sup. 2007) (noting that "the effect of an employer e-mail policy . . . is to have the employer looking over your shoulder each time you send an e-mail").

employer has a policy which clearly informs employees that company computers cannot be used for personal e-mail activity, and that they will be monitored. See United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use."); Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, \* 21 (D. Or. Sept. 15, 2004) ("when, as here, an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy."); Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002) ("But Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim."). In these cases, because the employee had no reasonable expectation of privacy, the employer did not need consent to search the employee's computer files.

This is not, however, a case where an employee was using an employer's computer or e-mail system, and then claimed that the e-mails contained on the employer's computers are private. Here, the employee - Fell - did not store any of the communications which his former employer now seeks to use against him on the employer's

computers, servers, or systems; nor were they sent from or received on the company e-mail system or computer. These e-mails were located on, and accessed from, third-party communication service provider systems. There is not even an implication that Fell's personal e-mail accounts were used for PPBC work, or that PPBC paid or supported Fell's maintenance of those accounts. See, e.g., Rozell v. Ross-Holst, No. 05 Civ. 2936 (JGK) (JCF), 2006 WL 163143, \*2-3 (S.D.N.Y. Jan. 20, 2006) (ordering production of e-mails taken from a personal third-party communication service provider account, which served as a back-up for work related communications). Furthermore, there is nothing in the PPBC policy that even suggests that if an employee simply views a single, personal e-mail from a third party e-mail provider, over PPBC computers, then all of the his personal e-mails on whatever personal e-mail accounts he uses, would be subject to inspection. In short, this case is distinguishable from those cases which hold that employees have no expectation of privacy in e-mails sent from or received and stored on the employer's computers.

Even in cases involving an employer's search of an employee's work computer, courts have held that, under certain circumstances, employees have a reasonable expectation of privacy in the contents of their work computer. For example, in Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001), the Second Circuit held that an employee had a reasonable expectation of privacy in the contents of

his computer where the employee occupied a private office with a door, had exclusive use of the computer in his office, and did not share use of his computer with other employees or the public, notwithstanding the fact that there was a policy which "prohibited 'using' state equipment 'for personal business.'" In Leventhal, there was no clear policy or practice regarding regular monitoring of work computers; technical staff conducted infrequent and selective searches for maintenance purposes only. See id.

In Curto v. Medical World Communications, No. 03 Civ. 6327 (DRH (MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006), the employer hired a forensic consultant to restore portions of the computer files that the employee had deleted, nearly two years earlier, from a home-based work computer, including e-mails of communications with the employee's lawyer. See id. at \*1. Even though the computer belonged to the employer, and the employer had a policy that warned employees they had no reasonable expectation of privacy in "anything they create, store, send, or received on the computer, or through the Internet or any computer network," the employee successfully asserted attorney-client privilege over those e-mails, in part because she had a reasonable expectation of privacy in a home-computer which was not connected to the employer's network. See id. at \*8.

And, in a recent case from the Ninth Circuit Court of Appeals, in which violations of both the SCA and the Fourth Amendment were



alleged, that court held that a police officer had a reasonable expectation of privacy in text messages sent using a city-owned pager. See Quon v. Archwireless, \_\_ F.3d \_\_, No. 07-55282, 2008 WL 2440559, \*13 (9th Cir. June 18, 2008) (concluding that "a reasonable juror could conclude . . . that plaintiff expected that his call to his wife would be private, and that expectation was objectively reasonable").

Here, Fell had a subjective belief that his personal e-mail accounts, stored on third-party computer systems, protected (albeit ineffectively) by passwords, would be private. That expectation of privacy was also reasonable, as nothing in PPBC's policy suggests that it could extend beyond Plaintiffs' own systems, and beyond the employment relationship. Furthermore, there is no evidence that PPBC's policy was clearly communicated to its employees, or that it was consistently enforced in a manner that would have alerted employees to the possibility that their private e-mail accounts, such as Hotmail, could also be accessed and viewed by their employer.

Because Fell had a reasonable expectation of privacy in his e-mail accounts, Brenner could only be authorized to access those accounts if Fell had given consent. She argues that Fell gave her implied consent to search his e-mails because he left his login information stored on PPBC's computers where it could be discovered

and used by Brenner. The Court does not accept Plaintiffs' argument.

There is no sound basis to argue that Fell, by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails, no less the e-mails in his two other accounts. If he had left a key to his house on the front desk at PPBC, one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings. And, to take the analogy a step further, had the person rummaging through the belongings in Fell's house found the key to Fell's country house, could that be taken as authorization to search his country house. We think not. The Court rejects the notion that carelessness equals consent. See Lipin v. Bender, 193 A.D.2d 424, 426, 597 N.Y.S.2d 340, 341 (1st Dep't 1993) (rejecting the argument that because documents "had been left unsecured, directly in front of the plaintiff, in a public area, . . . plaintiff had been 'invited' to read the documents").

Implied consent, at a minimum, requires clear notice that one's conduct may result in a search being conducted of areas which the person has been warned are subject to search. Cf. United States v. Workman, 80 F.3d 688, 694 (2d Cir. 1996) (holding that a posted sign and an inmate handbook, providing notice that telephone calls would be monitored, together with inmate's "plain awareness

that his conversations were subject to monitoring," amounted to implied consent to surveillance); United States v. Amen, 831 F.3d 373, 378-79 (2d Cir. 1987) (prisoners gave implied consent to interception of telephone calls because they were on notice from at least four sources, including actual direct notice); Sec. and Law Enforcement Employees v. Carey, 737 F.2d 187, 202 n.23 (2d Cir. 1984) (noting that an important consideration in determining whether a person has consented to being searched is "evidence that the person had knowledge of the right to refuse to give consent;" and rejecting the argument that correction officers consented to being strip-searched "merely by accepting employment and by receiving [a] rule book [giving notice that the Department's employees, while on correctional facility property, were subject to being searched]"); Anobile v. Pelligrino, 303 F.3d 107, 124-25 (2d Cir. 2002) (rejecting an assertion that racetrack employees, by signing a license with a "a blanket waiver of the right to object to any future searches," gave an effective consent to search their dormitory rooms, because "there [was] no evidence demonstrating that the plaintiffs were aware of their right to refuse to give consent to this unconstitutional search or indeed whether they could refuse and still obtain employment").

In this case, Fell only had notice that PPBC's computers could be searched for evidence of personal e-mail use, not that his Hotmail, Gmail, or WFBC e-mail accounts would also be searched. He

was also never given the opportunity to refuse Brenner any authorization to search his e-mails. At most, one could argue that Fell have consented to Brenner viewing his password. But he did not consent to her to using it. Absent clear knowledge of the extent of what could be searched, and the opportunity to refuse or withdraw his consent, the Court rejects Plaintiffs' argument that Fell gave implied consent to Brenner to search his Hotmail account simply by leaving his password on her computer.

Even less sustainable is the proposition that correctly "guessing" a person's password, as Brenner did, amounts to authorization to access all accounts which use that password. Were that the case, computer hackers across the country could escape liability for breaking into computer systems by correctly "guessing" the codes and passwords of their victims. This absurd result stands in direct conflict with the entire purpose of the SCA and basic principles of privacy. See In re DoubleClick, 154 F. Supp. 2d at 507.

The Court is convinced that Fell accessed his Hotmail account at some point when he was working at PPBC, and left his username and password stored on PPBC's computer. Otherwise, Brenner could not have obtained Fell's password, thereby making it possible for her to access his Hotmail account.<sup>9</sup> Nonetheless, the Court

---

<sup>9</sup> Defendants' suggestion that Brenner used a keystroke logging program is rank speculation, and, even if it were true, would only confirm that Fell entered his Hotmail password into

concludes that Brenner's access to Fell's Hotmail account violated the SCA and Fell's privacy. While Fell arguably "authorized" access to any e-mails which he viewed and saved on PPBC's computers, Brenner was not authorized to access those e-mails directly from Fell's Hotmail account, and was clearly not authorized to access e-mails from Fell's Gmail and WFBC accounts.

## II. Privilege and the Crime-Fraud Exception

Independent of whether the e-mails should be precluded because they were improperly secured, Defendants also assert that certain of these e-mails should be precluded, and they should be returned, because they are subject to the attorney-client privilege.

Plaintiffs' respond that the e-mails in question are not privileged communications. Plaintiffs also argue that Fell forfeited any right of privacy to all of his e-mails because those e-mails were in furtherance of what Plaintiffs describe as "civil and criminal misconduct." (Plaintiffs' Memorandum of Law in Opposition to the Motion to Preclude Use of E-mails ("Pls.' Mem."), at 9.) Thus, Plaintiffs invoke the crime-fraud exception to confidentiality, normally applicable to attorney-client privilege claims, and assert that Fell forfeited his right to privacy in all of his e-mails, including, but not limited to, e-mails covered by the attorney-client privilege.

---

PPBC's computers to access his Hotmail account.

The attorney-client privilege affords confidentiality to communications among clients and their attorneys, for the purpose of seeking and rendering an opinion on law or legal services, or assistance in some legal proceeding, so long as the communications were intended to be, and were in fact, kept confidential. See United States v. Int'l Bhd. of Teamsters, 119 F.3d 210, 214 (2d Cir. 1997); United States v. Doe (In re Six Grand Jury Witnesses), 979 F.2d 939, 943 (2d Cir. 1992); John Doe Corp. v. United States (In re John Doe Corp.), 675 F.2d 482, 487-88 (2d Cir. 1982); Bank Brussels Lambert v. Credit Lyonnais (Suisse) S.A., 160 F.R.D. 437, 441 (S.D.N.Y. 1995) (citing United States v. United Shoe Mach. Corp., 89 F. Supp. 357, 358-59 (D. Mass. 1950)). The privilege is among the oldest of the common law privileges and "exists for the purpose of encouraging full and truthful communication between an attorney and his client." In re von Bulow, 828 F.2d 94, 100 (2d Cir. 1987); accord United States v. Bilzerian, 926 F.2d 1285, 1292 (2d Cir. 1991). However, because the privilege "stands as an obstacle of sorts to the search for truth," it must be applied "only to the extent necessary to achieve its underlying goals." XYZ Corp. v. United States (In re Keeper of the Records), 348 F.3d 16, 22 (1st Cir. 2003); see also Salomon Bros. Treasury Litig. v. Steinhardt Partners (In re Steinhardt Partners), 9 F.3d 230, 235 (2d Cir. 1993) (finding that the privilege does not apply in situations where the client's conduct does not serve to "improve[]

the attorney-client relationship") (quoting Permian Corp. v. United States, 665 F.2d 1214, 1221 (D.C. Cir. 1981)). Thus, in order to merit protection, the "predominant purpose" of the communication must be to render or solicit legal advice, as opposed to business or policy advice. See In re County of Erie, 473 F.3d 413, 420 (2d Cir. 2007). Finally, "the burden of establishing the existence of an attorney-client privilege, in all of its elements, rests with the party asserting it." United States v. Doe (In re Grand Jury Proceedings), 219 F.3d 175, 182 (2d Cir. 2000) (quoting Int'l Bhd. of Teamsters, 119 F.3d at 214).

The attorney-client privilege is waived if the holder of the privilege voluntarily discloses or consents to disclosure of any significant part of the communication to a third party or stranger to the attorney-client relationship. See In re Grand Jury Proceedings, No. M-11-189 (LAP), 2001 WL 1167497, at \*7 (S.D.N.Y. Oct. 3, 2001); In re Kidder Peabody Sec. Litig., 168 F.R.D. 459, 468 (S.D.N.Y. 1996). Finally, a party who seeks to uphold the privilege must take affirmative measures to maintain the confidentiality of attorney-client communications. See In re Steinhardt Partners, 9 F.3d at 235; In re von Bulow, 828 F.2d at 100; In re Horowitz, 482 F.2d 72, 82 (2d Cir. 1973).

#### A. E-mails Protected by Attorney-Client Privilege

Defendant claims that E-mails 12, 13, 14, and 28 are protected by the attorney-client privilege. E-mail 12, though referred to by

the parties, was not provided with Defendants' motion papers. Defendants' counsel represents that it is an e-mail sent to Fell by a legal assistant at Fox Rothschild, the law firm representing Defendants. E-mail 13 was sent to Fell from a paralegal at Fox Rothschild, merely transmitting WFBC's employer ID number; attached is correspondence from the IRS. E-mail 14, from the same paralegal, indicates that WFBC's Articles of Organization were filed with the State of New York, and the Articles are attached. E-mail 28 is from an attorney at Fox Rothschild, and appears to be printed from Fell's "sent" file because the first part of the e-mail is a message from Fell to the attorney, as the end of a chain of back-and-forth e-mails from the same attorney. The e-mail contains advice about how to handle telephone calls from Brenner.

E-mails 13 and 14, sent to Fell from a paralegal at Fox Rothschild, are not communications seeking or rendering an opinion on law or legal services, and the information they contain is business information that is a matter of public record. The fact that the e-mails contain a warning indicating they contain "PRIVILEGED AND CONFIDENTIAL INFORMATION," does not transform them from non-privileged communications into privileged communications. See In re Grand Jury Proceedings, 2001 WL 1167497, at \*10 ("[T]he determination of whether a document is privileged does not depend upon . . . a privilege legend."). The Court therefore concludes that E-mails 13 and 14 are not privileged.



Defendants have not met their burden of demonstrating that E-mail 12 should be protected by the attorney-client privilege. This e-mail has not been provided to the Court for review, and the description provided in Defendants' memorandum of law is far too vague, and simply makes the conclusory assertion that it is subject to attorney-client privilege. Accordingly, the Court concludes that E-mail 12 is not privileged. See Fed. R. Civ. P. 26(b)(5)(A)(ii) ("the party must . . . describe the nature of the documents, communications, . . . and do so in a manner that . . . will enable other parties to assess the claim").

E-mail 28 is different. That e-mail is actually a series of communications, sent a month after Fell left PPBC, in which Fell, using his Hotmail account, sought advice from a Fox Rothschild attorney about how to handle telephone calls from Brenner. The attorney responds by providing advice and seeking additional information. Fell then responds with the additional information, and the attorney again provides specific legal advice. The communication ends with Fell thanking the attorney for the advice.

The Court concludes that this e-mail is protected by attorney-client privilege. It was clearly conveying information and legal advice, as well as the attorney's thoughts and impressions about the strengths of Fell's, and the other Defendants', legal position. There is some question, however, about the measures Fell took to keep the communications confidential, and whether it was

objectively reasonable for him to expect that his communications would be kept private.

On the one hand, according to his affidavit, Fell was using his own personal home computer to communicate with his attorney on a private e-mail account. It is generally accepted that lawyers and clients may communicate confidential information through unencrypted e-mail and reasonably maintain an expectation that the communications are private and confidential. See In re Asia Global Crossing, 322 B.R. at 256 (citing N.Y. C.P.L.R. § 4548 (McKinney 1999), stating that a privileged communication does not lose its privilege for the sole reason it was sent by e-mail)); cf. In re County of Erie, 473 F.3d at 422 (finding e-mails between county attorney and sheriff's office, sent with the predominant purpose of legal advice, were privileged so long as they were not shared with others); Geer v. Gilman Corp., No. 06 Civ. 889 (JBA), 2007 WL 1423752, \*4 (D. Conn. Feb. 12, 2007) ("[P]laintiff's attorney-client privilege in communications with her counsel was not waived by virtue of her having used her fiance's computer and e-mail address . . . [because] plaintiff took affirmative steps to maintain the confidentiality of the attorney-client communications.").

On the other hand, Fell left his Hotmail account vulnerable to the prying eyes of other parties by leaving his password stored on

PPBC's computer, and possibly by giving his login and password information to a PPBC employee.

Nonetheless, the Court has already concluded above that Fell had a reasonable subjective and objective belief that his communications would be kept confidential - and this includes his communications with his attorney. Even if Fell was fully aware of Plaintiffs' policy concerning e-mail, there is nothing in that policy that would have alerted him that, after he left Plaintiffs' employ, Brenner might search his personal e-mails sent through his personal computer, and stored on his personal internet providers' systems. Although Fell ultimately failed to properly protect his Hotmail password, there is no evidence that leaving it on PPBC's computers was anything but inadvertent. Thus, it remained reasonable for him to expect that the contents of his personal e-mails, particularly those written and sent after his employment at PPBC had ended, would be kept private when he sought the advice of his attorney. See In re County of Erie, 473 F.3d at 422; Geer v. Gilman Corp., 2007 WL 1423752, at \*4.

However, finding E-mail 28 is protected by the attorney-client privilege does not end the inquiry. Plaintiffs also argue that the privilege should be overcome based on the crime-fraud exception.

B. The Crime-Fraud Exception

The protections of the attorney-client privilege may be lost if the crime-fraud exception applies. "[T]he purpose of the

crime-fraud exception to the attorney-client privilege [is] to assure that the 'seal of secrecy,' between lawyer and client does not extend to communications 'made for the purpose of getting advice for the commission of a fraud' or crime." United States v. Zolin, 491 U.S. 554, 562-563, 109 S. Ct. 2619, 2626 (1989); see also In re John Doe, Inc., 13 F.3d 633, 636 (2d Cir. 1994) ("The crime-fraud exception strips the privilege from attorney-client communications that 'relate to client communications in furtherance of contemplated or ongoing criminal or fraudulent conduct.'" (quoting In re Grand Jury Subpoena Duces Tecum Dated September 15, 1983, 731 F.2d 1032, 1038 (2d Cir. 1984))).

"A party wishing to invoke the crime-fraud exception must demonstrate that there is a factual basis for a showing of probable cause to believe that a fraud or crime has been committed and that the communications in question were in furtherance of the fraud or crime." United States v. Jacobs, 117 F.3d 82, 87 (2d Cir. 1997). It is not enough to show merely that privileged communications "might provide evidence of a crime or fraud." In re Richard Roe, Inc., 168 F.3d 69, 71 (2d Cir. 1999). "Rather, the communication itself must have been in furtherance of a fraud or crime and must have been intended to facilitate the fraud or crime." Shahinian v. Tankian, 242 F.R.D. 255, 258 (S.D.N.Y. 2007) (citing Jacobs, 117 F.3d at 88).

1. Application to E-mail 28

Having reviewed the contents of E-mail 28, the Court concludes that there is no evidence that it was sent in furtherance of a fraud or crime. The communication clearly addresses the legal issues which Fell and other Defendants face, and the advice is limited to addressing those legal issues, and indicates how Fell and other Defendants should respond to Brenner, with whom a legal conflict had arisen. The fact that the communication arose in the larger context of the Defendants' attempt to set up a competing business, and discusses matters which might, in Plaintiffs' eyes, constitute past criminal or fraudulent actions, does not transform this particular communication into one which furthers a crime or fraud. Accordingly, the Court concludes that E-mail 28 is protected by the attorney-client privilege, should be precluded from use by Plaintiffs, and should be returned to Defendants. Further, Plaintiffs should certify that all copies have been returned or destroyed. See Fed. R. Civ. P. 26(b)(5)(B).

## 2. Application to All E-mails

Plaintiffs' crime-fraud exception argument is not limited, however, to only those e-mails for which attorney-client privilege was asserted. Plaintiffs also ask the Court to extend the principles underlying the crime-fraud exception to all of the e-mails in order to justify, and thereby excuse, Brenner's wrongful access to Fell's e-mail accounts. The Court declines to do so.

First, Plaintiffs' have not presented any authority for

extending the crime-fraud exception beyond the borders of its standard application to material covered by the attorney-client privilege. Second, had Brenner waited and acted appropriately, she would have had access to all of Fell's e-mails, as well as all of the other Defendants' e-mails, in the normal course of pre-trial discovery. While Brenner's fears that Defendants might attempt to conceal evidence cannot, in this case, be written off as unfounded paranoia, neither federal law nor the Federal Rules of Civil Procedure can be ignored simply because a party believes herself to be wronged by the actions of a dishonest person. If the Court were to adopt Plaintiffs' suggestion, the crime-fraud exception would engulf all of the rules designed to ensure orderly and legal discovery of evidence, and could be invoked to justify any party's resort to illegal, extra-judicial measures to secure evidence. Accordingly, the Court rejects Plaintiffs' suggestion that the crime-fraud exception should excuse Brenner's violations of the SCA.

### III. Spoliation

Defendants' final argument is that Plaintiffs' initial production of the e-mails, with their print date obscured, amounts to spoliation of evidence, justifying sanctions, including preclusion. The Court does not agree.

"Spoliation is the destruction or significant alteration of evidence, or failure to preserve property for another's use as

evidence in pending or reasonably foreseeable litigation.'" Allstate Ins. Co. v. Hamilton Beach/Proctor Silex, Inc., 473 F.3d 450, 457 (2d Cir. 2007) (quoting West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999)). Typically, when evidence is spoiled, a party requests dismissal or an "adverse inference" instruction to counteract the fact that the evidence is no longer available. See West, 167 F.3d at 780 (noting that dismissal is not the only sanction for spoliation, and that other sanctions, including jury instructions, also serve to vindicate the prejudice suffered by a party due to spoliation); cf. Residential Funding Corp. v. Degeorge Fin. Corp., 306 F.3d 99, 106 (2d Cir. 2002) (noting that "adverse inference instruction[s] [are] usually [] employed in cases involving spoliation of evidence"). This is not, however, a typical case, because the evidence is available in its original form. Accordingly, neither of these severe sanctions - dismissal or an adverse inference instruction - are commensurate or appropriate sanctions.

When the nature of the breach is non-production of evidence, as opposed to actual destruction or significant alteration, a district court "has broad discretion in fashioning an appropriate sanction". Residential Funding Corp., 306 F.3d at 107. In Residential Funding, a case similar to this case, the plaintiff did not destroy "the e-mails on the back-up tapes. Rather, [the plaintiff] failed to produce the e-mails in time for trial." Id.

at 106. The Second Circuit remanded the case, and instructed the district court to consider lesser sanctions, including awarding costs, if it determined that the defendant was not prejudiced by the delay. See id. at 112. Thus, the harm caused by delay in production is a relevant factor in determining sanctions, if a court determines that sanctions are warranted. See West, 167 F.3d at 780 (noting that addressing prejudice is an important aim of sanctions imposed for abuses of discovery).

In this case, the original e-mails were not destroyed or altered, and Defendants inspected them prior to making their final argument to the District Court, regarding the motion for a preliminary injunction. The date the e-mails were printed was made known to Defendants and the Court before the preliminary injunction hearing. Thus, at most, Defendants could argue that production was delayed. However, Defendants were not harmed by the delay, as they were not prevented from addressing the evidence or making any arguments related to the e-mails - including the current preclusion motion.<sup>10</sup> Cf. Residential Funding Corp., 306 F.3d at 107.

This is not to say that altering evidence, as Plaintiffs did, and delaying production of unaltered evidence until the day of the

---

<sup>10</sup> Defendants only claim as to the relevance that the obscured dates would have to their claims is that the dates the e-mails were printed might show contemporaneous "interception" under the ECPA. However, the Court has concluded that the ECPA does not apply to delivered e-mails, and the date the e-mails were printed is not relevant to the analysis because only delivered e-mails could be printed.



hearing, is excusable. However, Plaintiffs' current counsel has represented that prior counsel provided the e-mails in the state court litigation, and was responsible for obscuring the dates. (See Tr. at 14-15.) His explanation for doing so is unknown. Accordingly, the Court finds that obscuring the dates, alone, does not amount to spoliation warranting the imposition of sanctions, let alone total preclusion.

#### IV. Remedies

##### A. Authority to Impose Sanctions

The SCA allows a person who is "aggrieved by any violation of this chapter" to obtain "such relief as may be appropriate" in a civil cause of action. 18 U.S.C. § 2707(a). The statute further provides in sub-section (b): "appropriate relief includes - (1) such preliminary and other equitable or declaratory relief as may be appropriate; (2) damages under subsection (c); and (3) a reasonable attorney's fee and other litigation costs reasonably incurred." Id. However, Defendants have not asserted a claim under the SCA; therefore, these provisions do not define or limit the sanctions the Court may impose in this case. Rather, Defendants appeal to the Court's inherent equitable authority to fashion appropriate sanctions for Brenner's actions.

Federal courts do have "inherent 'equitable powers of courts of law over their own process, to prevent abuses, oppression, and injustices,'" International Prods. Corp. v. Koons, 325 F.2d 403,

408 (2d Cir. 1963) (quoting Gumbel v. Pitkin, 124 U.S. 131, 144, 8 S. Ct. 379 (1888)); see also Schlaifer Nance & Co., Inc. v. Estate of Warhol 742 F. Supp. 165, 166 (S.D.N.Y. 1990) (quoting Koons). Courts may impose sanctions and rely upon their inherent authority even "where the conduct at issue is not covered by one of the other sanctioning provisions." Chambers v. NASCO, Inc., 501 U.S. 32, 50, 111 S. Ct. 2123, 2135 (1991). Furthermore, a district court may resort to its "inherent power to fashion sanctions, even in situations similar or identical to those contemplated by [a] statute or rule." DLC Mgmt. Corp. v. Town of Hyde Park, 163 F.3d 124, 136 (2d Cir. 1998) (citing Chambers).

In this situation, the sanctions available under the Federal Rules of Civil Procedure are not directly applicable, since Brenner's misconduct occurred prior to the filing of the litigation and outside the normal discovery process, and did not violate any court orders. See Fayemi v. Hambrecht and Quist, Inc., 174 F.R.D. 319, 325 (S.D.N.Y. 1997) (concluding that the Federal Rules of Civil Procedure did "not provide the authority for regulating the use of information obtained by a party independent of the discovery process"). Nonetheless, as the court in Fayemi found, pursuant to "its inherent equitable powers to sanction a party that seeks to use in litigation evidence that was wrongfully obtained," the court may preclude the use of stolen evidence in litigation, notwithstanding the fact that it would have been otherwise

discoverable. See id. at 325-26.

In another analogous case, Herrera v. The Clipper Group, L.P., Nos. 97 Civ. 560 & 561 (SAS), 1998 WL 229499 (S.D.N.Y. May 6 1998), the defendant sought to preclude the plaintiff from using at trial documents improperly obtained outside the discovery process. Relying on its inherent authority, the court concluded that the plaintiff acted in bad faith and imposed sanctions, consisting of payment of costs and fees. See id. at \*3. However, because the plaintiff could have properly obtained the evidence through the discovery process, the court declined to preclude the use of the evidence. See id. at \*5. The court was also hesitant to provide the defendants with a "windfall" strategic advantage at trial. See id.

#### B. Bad Faith

The Second Circuit "has required a finding of bad faith for the imposition of sanctions under the inherent power doctrine." Herrera, 1998 WL 229499, at \*4 (citing United States v. Int'l Bhd. of Teamsters, 948 F.2d 1338, 1345 (2d Cir. 1991)). The Court concludes that Brenner acted in bad faith. The Court understands Brenner's impulse to unearth evidence of her disloyal employees' betrayal, after having reason to believe they had stolen important business documents and plans, and after they opened up a competing business after leaving PPBC. This is particularly true in light of Belliard's decision to invade her office, shred his non-compete

agreement, and take other actions which caused Brenner to believe that he stole PPBC's client list, including e-mail addresses and telephone numbers.

But it is precisely this conduct which is the subject of this litigation and for which, if proved, Brenner has adequate legal remedies. Her actions - accessing of Fell's Hotmail account, and using that access to open his Gmail account, and then resorting to "guessing" a password in order to gain access to Fell's WFBC account - violated federal law and offend general notions of personal privacy. Furthermore, her use of that information in this litigation taints the judicial process. Thus, even though Brenner's improper actions took place prior to the filing of the litigation, the fruits of Brenner's improper conduct have been heavily relied upon by Plaintiffs in pleading and arguing the merits of their case. The Court may therefore fashion sanctions for Brenner's wrongful access to Fell's personal e-mail accounts. See Herrera, 1998 WL 229499 at \*5.

#### C. Sanctions

Defendants seek the complete preclusion of all of the e-mails, including their use in support of motions, at trial, and even for impeachment purposes. There are a variety of options, however, that are available to the Court.

On the mild side of the spectrum, the Court could preclude the use of e-mails obtained from Fell's accounts, but not e-mails

properly obtained in the course of discovery from other Defendants or parties - even if the permitted e-mails might, in actuality, be the same as those precluded. Although this would amount to imposing almost no sanction, it recognizes the fact that the evidence would be otherwise discoverable.<sup>11</sup>

However, the notion that the evidence would be otherwise discoverable also cuts in the other direction. Had Brenner allowed the litigation process to move forward, and not violated federal law to by-pass the rules of discovery, she could have properly obtained the e-mails in question. Moreover, many of the e-mails in issue were authored by other people and sent to Fell, and in those cases, those individuals were also aggrieved by Brenner's intrusion into Fell's e-mail accounts. Permitting precluded e-mails to be admitted from other sources would therefore fail to take into account the fact that Brenner's actions also violated the privacy rights of everyone with whom Fell communicated. As discussed, parties should not be excused from complying with the law and following the rules because of outrage, legitimate or otherwise, over another party's actions.

---

<sup>11</sup> In the Fourth Amendment context, the Independent Source Exception and the Inevitable Discovery Exception both allow evidence otherwise illegally obtained to be admissible in a criminal case if it could and would have been lawfully obtained anyway. See Murray v. United States 487 U.S. 533 (1988); Nix v. Williams, 467 U.S. 431 (1984).

On the harsh side of the spectrum, the Court could completely preclude use of the e-mails for all purposes, in any context, regardless of whether they could be secured from some other source. This option could be tempered, however, by allowing the e-mails to be used for impeachment purposes.<sup>12</sup> Thus, while precluding the use of the e-mails as affirmative evidence, the Court would not permit Fell or others to testify falsely, or open the door to a line of testimony that is contradicted by the e-mails, knowing that the e-mails could not be used to impeach or rebut their testimony. Additionally, if there are e-mail chains between Defendants that merely contain a precluded e-mail from Fell, the chain of conversation would be admissible, and only the precluded e-mail would be redacted.

Alternatively, selective preclusion of the e-mails could also be accomplished by carving out categories of e-mails. For example, e-mails dated before March 16, 2008, the last date of Fell's employment with PPBC, could be allowed in evidence, but later e-mails could be precluded; in fact, Defendants recognized this categorical distinction during oral argument. (See Tr. at 27.)

---

<sup>12</sup> Defendants urge the Court to reject an impeachment exception to preclusion, and cite to a Sixth Circuit case which explicitly holds that the ECPA does not provide for one. See United States v. Wuliger, 981 F.2d 1497, 1506 (6th Cir. 1992). As the Court has determined that the ECPA does not apply, and the remedies available under the SCA are left to the discretion of the Court, and as this Court is acting pursuant to its inherent authority, nothing prevents the Court from allowing an impeachment exception.

Alternatively, only Gmail and WFBC account e-mails could be precluded, but not Hotmail account e-mails, since Fell clearly accessed his Hotmail account on Plaintiffs' computers and left his Hotmail password on PPBC's computers. Limited preclusion, such as one based on the date on which the e-mail was written (for example, e-mails sent after Fell left PPBC), or the type of account from which it was retrieved (e-mails from the Gmail or WFBC accounts), might be justified by the fact that both parties appear to have "unclean hands;" such a sanction would punish Brenner's wrongful acts, while limiting an evidentiary "windfall" going to Defendants, who also engaged in wrongful behavior. See Fayemi, 174 F.R.D. at 326 (permitting evidence that would otherwise have been precluded because of the "unclean hands" of the aggrieved party); Herrera, 1998 WL 229499, at \*5 (declining to grant opposing party an evidentiary "windfall").

The problem with this alternative is that, ultimately, there is little justifiable basis to distinguish the e-mails according to their source or date. Brenner was not authorized to access any of Fell's e-mails directly from accounts maintained by third-party electronic communication service providers. Thus, while it is possible to create categories of e-mails, it is difficult to justify why one category should be precluded, while another should be admissible.

Finally, the Court could impose financial sanctions such as

payment of the costs and fees incurred in bringing the instant motion.<sup>13</sup> These could be imposed in conjunction with a preclusion sanction, or, as the court did in Herrera, as an alternative to preclusion. Monetary sanctions, as opposed to full preclusion, would serve the Court's interest in favoring full disclosure of evidence. In the context of lifting a protective order, the Second Circuit has noted that "full disclosure of all evidence that might conceivably be relevant [is an] objective represent[ing] the cornerstone of our administration of civil justice." Martindell v. International Tel. and Tel. Corp., 594 F.2d 291, 295 (2d Cir. 1979).

The disadvantage of imposing a monetary sanction is that it does not really address the underlying injury to Fell's privacy. Furthermore, preclusion of the e-mails is the remedy most compatible with maintaining the integrity of the litigation process. As one court noted: "The [c]ourt is concerned with preserving the integrity of this judicial proceeding. What matters is balancing the scales. That can be done by prohibiting [a party]

---

<sup>13</sup> Defendants have not specified precisely the costs or fees they are seeking. The SCA permits awarding fees and costs, and, if the violation was willful, the imposition of punitive damages. See 18 U.S.C. § 2707(c); see also Wyatt Technology Corp., 2006 WL 5668246, at \*9 (awarding punitive damages to a counter-claimant under the SCA, because the plaintiff accessed the defendant's personal e-mail on a private foreign server, monitored the personal e-mail account, and did not obtain the defendant's authorization to do so).



from making any use of the [wrongfully obtained] documents . . . ."

In re Shell Oil Refinery, 143 F.R.D. 105, 108-09 (E.D.La. 1992).

#### CONCLUSION

In fashioning a remedy pursuant to its inherent equitable powers, the Court has a great deal of discretion. See DLC Mgmt., 163 F.3d at 136 (upholding sanctions imposed by Magistrate Judge pursuant to the court's inherent equitable authority) (citing Sassower v. Field, 973 F.2d 75, 80-81 (2d Cir. 1992)). The selection of a remedy for Brenner's actions is not, however, an easy task. Brenner wrongfully obtained Fell's e-mails, and her actions amount to a violation of the SCA. But the Court also recognizes that Brenner was reacting to what she perceived as Defendants' betrayal, theft of her property, and breaches of their fiduciary duties. Thus, the parties seeking equitable relief, Defendants, stand accused of having extremely unclean hands themselves. Furthermore, although Brenner's actions may have given Plaintiffs an advantage at the outset of this litigation, they did not, in the end, give them an advantage over Defendants they would not otherwise have had - all of the e-mails at issue here, except the one protected by the attorney-client privilege, would have been secured through the normal discovery process.

Nevertheless, at this stage in the litigation, the Court has not resolved the merits of Plaintiffs' claims, which will determine just how much dirt is on Defendants' hands. While the day may come

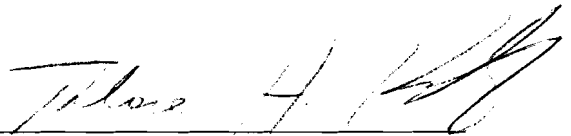
when Defendants will face the consequences for their alleged misconduct, Brenner's wrongdoing has been established, and should not be counter-balanced by, as-yet, unproven allegations of wrongdoing on the part of Defendants. Accordingly, the imposition of sanctions against Plaintiffs is justified.

In the end, the one thing that should remain unsullied is the integrity of the judicial process. In this Court's view, that integrity is threatened by admitting evidence wrongfully, if not unlawfully, secured. See REP MCR Realty, L.L.C. v. Lynch, 363 F. Supp. 2d 984, 1012 (N.D.Ill. 2005) ("Litigants must know that the courts are not open to persons who would seek justice by fraudulent means.") (quoting Pope v. Federal Exp. Corp., 138 F.R.D. 675, 683 (W.D.Mo. 1990)). Therefore, in light of the unique circumstances of this case, the Court recommends that the e-mails be precluded from use in the litigation, but not for impeachment purposes should Defendants open the door. The Court also recommends that Plaintiffs should return or destroy all copies of E-mail 28, and so certify.

Pursuant to 28 U.S.C. § 636(b)(1)(C) and Rule 72 of the Federal Rules of Civil Procedure, the parties shall have ten (10) days from service of this Report to file written objections. See also Fed. R. Civ. P. 6(a) and (d). Such objections shall be filed with the Clerk of the Court, with extra copies delivered to the chambers of the Honorable John H. Koeltl, United States District Judge, and to the chambers of the undersigned, Room 1660. Any

requests for an extension of time for filing objections must be directed to Judge Koeltl. Failure to file objections will result in a waiver of those objections for purposes of appeal. See Thomas v. Arn, 474 U.S. 140, 145, 106 S. Ct. 466, 470 (1985); Frank v. Johnson, 968 F.2d 298, 300 (2d Cir. 1992); Small v. Sec'y of Health & Human Servs., 892 F.2d 15, 16 (2d Cir. 1989).

Respectfully submitted,

  
\_\_\_\_\_  
THEODORE H. KATZ  
UNITED STATES MAGISTRATE JUDGE

Dated: August 22, 2008  
New York, New York